

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

GRAHAM, Robert, J.
Gowling Lafleur Henderson LLP
Suite 4900
Commerce Court West
Toronto, Ontario M5L 1J3
CANADA

Date of mailing (day/month/year) 06 July 2001 (06.07.01)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference T8466293WO	
International application No. PCT/CA01/00236	International filing date (day/month/year) 01 March 2001 (01.03.01)

1. The following indications appeared on record concerning:		
<input checked="" type="checkbox"/> the applicant	<input checked="" type="checkbox"/> the inventor	<input type="checkbox"/> the agent <input type="checkbox"/> the common representative
Name and Address PIDDUK, Patrick 267 Castlefield Avenue Waterloo, Ontario N2K 2M4 Canada	State of Nationality CA	State of Residence CA
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:		
<input type="checkbox"/> the person	<input checked="" type="checkbox"/> the name	<input type="checkbox"/> the address <input type="checkbox"/> the nationality <input type="checkbox"/> the residence
Name and Address PIDDUCK, Patrick 267 Castlefield Avenue Waterloo, Ontario N2K 2M4 Canada	State of Nationality	State of Residence
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
3. Further observations, if necessary: Correction in name.		
4. A copy of this notification has been sent to:		
<input checked="" type="checkbox"/> the receiving Office	<input checked="" type="checkbox"/> the designated Offices concerned	
<input checked="" type="checkbox"/> the International Searching Authority	<input type="checkbox"/> the elected Offices concerned	
<input type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:	

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer J. Leitao
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Best Available Copy

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 01 November 2001 (01.11.01)	
International application No. PCT/CA01/00236	Applicant's or agent's file reference T8466293WO
International filing date (day/month/year) 01 March 2001 (01.03.01)	Priority date (day/month/year) 01 March 2000 (01.03.00)
Applicant SPICER, Steven et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
 28 September 2001 (28.09.01)

☐ in a notice effecting later election filed with the International Bureau on:

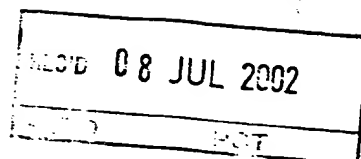
2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Cécile CHATEL (Fax 338.87.40) Telephone No.: (41-22) 338.83.38
---	---

PATENT COOPERATION TREATY

PCT



INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)


Applicant's or agent's file reference T8466293WO		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/CA01/00236	International filing date (day/month/year) 01/03/2001	Priority date (day/month/year) 01/03/2000
International Patent Classification (IPC) or national classification and IPC H04L12/24		
Applicant SPICER CORPORATION et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.
 - ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 28/09/2001	Date of completion of this report 05.07.2002
Name and mailing address of the international preliminary examining authority:  European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized officer Veen, G Telephone No. +31 70 340 3811



INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/CA01/00236

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, pages:

1-19 as originally filed

Claims, No.:

1-12 with telefax of 12/04/2002

Drawings, sheets:

1/5-5/5 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/CA01/00236

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-12
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-12
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-12
	No:	Claims	

2. Citations and explanations
see separate sheet

1 Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1.1 Claim 1

The closest prior art, represented by D1, discloses a method of interfacing a plurality of server computers with input and output devices at a plurality of user locations, using a switch.

It does not disclose, however, the aspect of providing a user with the address of a network resource specified by the user in terms of its alias name, depending on the user's configuration data and authorization level, as defined in independent claim 1. These features solve the problems of freeing users from the need to know more than a resource's alias name and enabling dynamic resource access control without having to reconfigure each terminal.

Therefore, the defined in claim 1 is not obvious, and claim 1 satisfies the requirements of Articles 33(2) and 33(3) PCT.

1.2 Claims 2-6

Claims 2-6 are dependent on claim 1 and therefore also meet the requirements of Articles 33(2) and 33(3) PCT.

1.3 Claim 7

Claim 7 defines the method implemented by the system of claim 1 and therefore also meets the requirements of Articles 33(2) and 33(3) PCT.

1.4 Claims 8-12

Claims 8-12 are dependent on claim 7 and therefore also meet the requirements of Articles 33(2) and 33(3) PCT.

2 Re Item VII

Certain defects in the international application

- 2.1** Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in D1 is not mentioned in the description, nor is D1 mentioned in the

description.

- 2.2 Contrary to the requirements of Rule 6.2(b) PCT, the technical features mentioned in the claims are not followed by reference signs relating to those features.
- 2.3 Contrary to the requirements of Rule 6.3(b) PCT, the claims have not been cast in the two-part form, with those features which in combination are part of the prior art (see D1) being placed in the preamble.

3 Re Item VIII

Certain observations on the international application

The last paragraph of the description ("The foregoing description ...") implies that the subject-matter for which protection is sought may be different from that defined by the claims, which results in lack of clarity of the claims (Article 6 PCT) when used to interpret them.

-20-

WE CLAIM:

1. A network resource control system for controlling communication between network terminals and network resources over a network, the network resource control system comprising:
a resource registry including resource records associated with the network resources, the resource records including configuration data for the network resources, each said configuration data including a resource alias name, a network address and a user authorization level for the associated network resource; and
an authorization server in communication with the resource registry for controlling network access to the network resources by the network terminals, the authorization server being configured for receiving from one of the network terminals user configuration data, and the resource alias name of one of the network resources, and for providing the one network terminal with the resource configuration data of the one network resource in accordance with a correspondence between the user configuration data and the user authorization level of the one network resource, the provided configuration data including the network address of the one network resource.
2. The network resource control system according to claim 1, wherein the user configuration data includes one of a network address associated with the one network terminal, and user authentication data associated with a user of the one network terminal.
3. The network resource control system according to claim 2, wherein the provided resource configuration data includes a password for accessing the one network resource.
4. The network resource control system according to claim 3, wherein the resource configuration data defines access rights to the resource records, and the network resource control system includes an administration server for dynamically controlling access to the network resources, the administration server being in communication with the resource registry and configured for receiving updates to the configuration data.

-21-

5. The network resource control system according to claim 2, wherein the one network resource comprises one of a printer, a facsimile machine, an image server and a file server.
6. The network resource control system according to claim 6, wherein the one network terminal comprises one of a personal computer and a wireless communications device.
7. A method for controlling communication between network terminals and network resources over a network, the method comprising the steps of:
 - providing a resource registry including resource records associated with the network resources, the resource records including configuration data for the network resources, each said configuration data including a resource alias name, a network address and a user authorization level for the associated network resource; and
 - facilitating communication by the network terminals with one of the network resources, the communication facilitating step comprising the steps of receiving from one of the network terminals user configuration data, and the resource alias name of one of the network resources, and providing the one network terminal with the resource configuration data of the one network resource in accordance with a correspondence between the user configuration data and the user authorization level of the one network resource, the provided configuration data including the network address of the one network resource.
8. The method according to claim 7, wherein the user configuration data includes one of a network address associated with the one network terminal, and user authentication data associated with a user of the one network terminal.
9. The method according to claim 8, wherein the provided resource configuration data includes a password for accessing the one network resource.
10. The method according to claim 9, wherein the resource configuration data defines access rights to the resource records, and the method includes the steps of receiving from a network

-22-

administrator a request for access to one of the resource records, verifying authorization for the access from the resource configuration data associated with the one resource record, and updating the resource configuration data for the one resource record in accordance with the verification.

11. The method according to claim 8, wherein the one network resource comprises one of a printer, a facsimile machine, an image server and a file server.

12. The method according to claim 11, wherein the one network terminal comprises one of a personal computer and a wireless communications device.

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference T8466293W0	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/CA 01/ 00236	International filing date (day/month/year) 01/03/2001	(Earliest) Priority Date (day/month/year) 01/03/2000
Applicant SPICER CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1
☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/CA 01/00236

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/24 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 22294 A (C C C GROUP PLC) 6 May 1999 (1999-05-06) page 3, line 18 -page 6, line 2 ---	1-8
X	US 5 987 611 A (FREUND GREGOR) 16 November 1999 (1999-11-16) claim 1 --- -/--	1-8

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *8* document member of the same patent family

Date of the actual completion of the international search

12 November 2001

Date of mailing of the international search report

20/11/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Veen, G

INTERNATIONAL SEARCH REPORT

International Application No

PCT/CA 01/00236

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>SITAO W ET AL: "USING DEVICE DRIVER SOFTWARE IN SCADA SYSTEMS" 2000 IEEE POWER ENGINEERING SOCIETY. WINTER MEETING. CONFERENCE PROCEEDINGS. SINGAPORE, JAN. 23-27, 2000, IEEE POWER ENGINEERING SOCIETY WINTER MEETING, NEW YORK, NY: IEEE, US, vol. 3 OF 4, 23 January 2000 (2000-01-23), pages 2046-2049, XP000967795 ISBN: 0-7803-5936-4 page 2046, right-hand column, paragraph 3 -page 2047, right-hand column, paragraph 1 -----</p>	3,7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/CA 01/00236

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9922294	A	06-05-1999	AU 9752798 A	17-05-1999
			CN 1277687 T	20-12-2000
			EP 1025490 A1	09-08-2000
			WO 9922294 A1	06-05-1999
<hr/>				
US 5987611	A	16-11-1999	NONE	
<hr/>				

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
7 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65769 A3

(51) International Patent Classification⁷: **H04L 12/24**,
29/06

(21) International Application Number: PCT/CA01/00236

(22) International Filing Date: 1 March 2001 (01.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2,299,824 1 March 2000 (01.03.2000) CA

(71) Applicant (for all designated States except US): **SPICER CORPORATION** [CA/CA]; 221 McIntyre Drive, Kitchener, Ontario N2R 1G1 (CA).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SPICER, Steven** [CA/CA]; 119 Champlaine Crescent, Kitchener, Ontario N2B 2Y7 (CA). **MARTIN, Christopher** [CA/CA]; 66

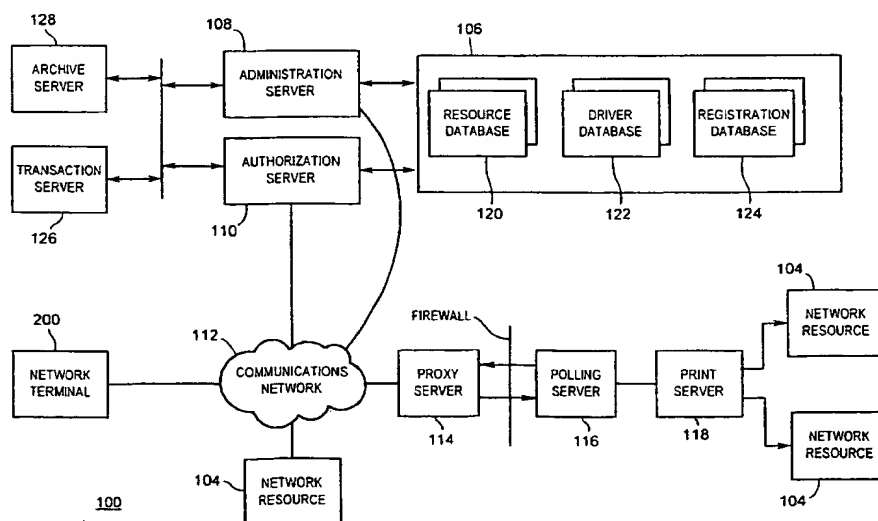
Mooregate Crescent, Apt. 1304, Kitchener, Ontario N2M 5E6 (CA). **COUTTS, Steven** [CA/CA]; 99 John Street, Waterloo, Ontario N2L 1C2 (CA). **KUHL, Larry** [CA/CA]; 686 Jacob Lane, Waterloo, Ontario N2V 1G9 (CA). **HOLLANDER, Brian** [CA/CA]; 99 Julia Crescent, Kitchener, Ontario N2E 3M7 (CA). **PIDDUCK, Patrick** [CA/CA]; 267 Castlefield Avenue, Waterloo, Ontario N2K 2M4 (CA). **VON HATTEN, Philip** [CA/CA]; 2240 Walker Road, New Hamburg, Ontario N0B 2G0 (CA). **LEHAN, Tim** [CA/CA]; 168 Samuel Street, Kitchener, Ontario N2H 1R1 (CA). **ONISCHKE, Mark** [CA/CA]; 220-150 Country Hills Drive, Kitchener, Ontario N2E 3H2 (CA). **GRASSICK, Clayton** [CA/CA]; 15 Cambrian Crescent, Winnipeg, Manitoba R3R 1Y3 (CA).

(74) Agents: **GRAHAM, Robert, J.** et al.: Gowling Lafleur Henderson LLP, Suite 4900, Commerce Court West, Toronto, Ontario M5L 1J3 (CA).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ.

[Continued on next page]

(54) Title: NETWORK RESOURCE CONTROL SYSTEM



(57) Abstract: A network resource control system allows network terminals to communicate with network resources, and includes a resource registry, an authorization server and an administration server. The resource registry includes resource records which are associated with the network resources and define at least a user access level for each network resource. The authorization server is in communication with the resource registry and controls network access to the network resources in accordance with the resource records. The administration server is in communication with the resource registry and provides controlled access to the resource records. The administration server receives user access control data from administrators of the network resources for incorporation into the resource records. Depending upon the user access control data received, the authorization server configures the network terminals for communication with the network resources.

WO 01/65769 A3



NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

Published:

— with international search report

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(88) Date of publication of the international search report:

28 February 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETWORK RESOURCE CONTROL SYSTEM

FIELD OF THE INVENTION

The present invention relates to a method and system for network management
5 system. In particular, the present invention relates to a method and system for
controlling access to network resources.

BACKGROUND OF THE INVENTION

Local area networks are widely used as a mechanism for making available computer
10 resources, such as file servers, scanners, and printers, to a multitude of computer
users. It is often desirable with such networks to restrict user access to the computer
resources in order to manage data traffic over the network and to prevent unauthorized
use of the resources. Typically, resource access is restricted by defining access
control lists for each network resource. However, as the control lists can only be
15 defined by the network administrator, it is often difficult to manage data traffic at the
resource level.

Wide area networks, such as the Internet, have evolved as a mechanism for providing
distributed computer resources without regard to physical geography. Recently, the
20 Internet Print Protocol ("IPP") has emerged as a mechanism to control access to
printing resources over the Internet. However, IPP is replete with deficiencies.

First, as IPP-compliant printing devices are relatively rare, Internet printing is not
readily available.
25

Second, although IPP allows user identification information to be transmitted to a
target resource, access to IPP-compliant resources can only be changed on a per-
resource basis. This limitation can be particularly troublesome if the administrator is
required to change permissions for a large number of resources.
30

Third, users must have the correct resource driver and know the IPP address of the
target resource before communicating with the resource. Therefore, if the device type
or the IPP address of the target resource changes, users must update the resource
driver and/or the IPP address of the resource. Also, if a user wishes to communicate

with a number of different resources, the user must install and update the resource driver and IPP address for each resource as the properties of each resource changes.

5 Fourth, access to IPP printers cannot be obtained without the resource administrator locating the resource outside the enterprise firewall, or without opening an access port through the enterprise firewall. Whereas the latter solution provides the resource administrator with the limited ability to restrict resource access, the necessity of opening an access port in the enterprise firewall exposes the enterprise network to the possibility of security breaches.

10

Consequently, there remains a need for a network resource control solution which allows resource owners to easily and quickly control resource access, which is not hindered by changes in device type and resource network address, which facilitates simultaneous communication with a number of target resources, and which does not expose the enterprise network to a significant possibility of security breaches.

15

SUMMARY OF THE INVENTION

According to the invention, there is provided a network resource control system and a method of network resource control which addresses at least one deficiency of the prior art network resource control systems.

20

The network resource control system, according to the present invention, allows network users to communicate with network resources, and comprises a resource registry, an authorization server and an administration server. The resource registry includes resource records which are associated with the network resources and define at least a user access level for each network resource. The authorization server is in communication with the resource registry and controls network access to the network resources in accordance with the resource records. The administration server is in communication with the resource registry and provides controlled access to the resource records.

25

30

The network resource control method, according to the present invention, facilitates communication between network users and network resources, and comprises the steps of (1) providing a resource registry including resource records associated with

the network resources, the resource records including user access control data; (2) receiving user access control data from administrators of the network resources for incorporation into the resource records; and (3) in accordance with the user access control data, configuring the network terminals for communication with the network resources.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiment of the invention will now be described, by way of example only, with reference to the drawings, in which:

10

Fig. 1 is a schematic view of the network resource control system, according to the present invention, showing the network terminals, the network resources, the resource registry, the authorization server, the administration server, the proxy server, and the polling server;

15

Fig. 2 is a schematic view one of the network terminals depicted in Fig. 1, showing the driver application for use with the present invention;

20

Fig. 3 is a schematic view of the format of the resource records comprising the resource database of the resource registry depicted in Fig. 1, showing the network address field, the resource type field, the user access level field, the resource information field, the pseudo-name field, the username/password field, and the driver identification field; and

25

Fig. 4 is a flow chart depicting the method of operation of the network resource control system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Turning to Fig. 1, a network resource control system, denoted generally as 100, is shown comprising a network terminal 200, a network resource 104, a resource registry 106, an administration server 108, and an authorization server 110. Typically, the network resource control system 100 comprises a plurality of network terminal 200, and a plurality of network resources 104, however for enhanced clarity of discussion, Fig. 1 only shows a single network terminal 200 and a single network resource 104.

The network resource control system 100 also includes a communications network 112 facilitating communication between the network terminals 200, the network resources 104, the administration server 108, and the authorization server 110. Preferably, the communications network 112 comprises a wide area network such as the Internet, however the network 112 may also comprise a local area network. Further, the network 112 need not be a land-based network, but instead may comprise a wireless network and/or a hybrid of a land-based network and a wireless network for enhanced communications flexibility.

Each network terminal 200 typically comprises a land-based network-enabled personal computer. However, the invention is not limited for use with personal computers. For instance, one or more of the network terminals 200 may comprise a wireless communications device, such as a wireless-enabled personal data assistant, or e-mail-enabled wireless telephone if the network 112 is configured to facilitate wireless data communication. In addition, the invention is not limited to only facilitating transmission of text data, but instead may be used to transmit image data, audio data or multimedia data, if desired.

As shown in Fig. 2, the network terminal 200 comprises a network interface 202, a user interface 204, and a data processing system 206 in communication with the network interface 202 and the user interface 204. Typically, the network interface 202 comprises an Ethernet network circuit card, however the network interface 202 may also comprise an RF antenna for wireless communication over the communications network 112. Preferably, the user interface 204 comprises a data entry device 208 (such as keyboard, microphone or writing tablet), and a display device 210 (such as a CRT or LCD display).

The data processing system 206 includes a central processing unit (CPU) 208, and a non-volatile memory storage device (DISC) 210 (such as a magnetic disc memory or electronic memory) and a read/write memory (RAM) 212 both in communication with the CPU 208. The DISC 210 includes data which, when loaded into the RAM 212, comprise processor instructions for the CPU 208 which define memory objects for allowing the network terminal 200 to communicate with the network resources 104 and the authorization server 110 over the communications network 112. The network

terminal 200, and the processor instructions for the CPU 208 will be discussed in greater detail below.

Typically, each network resource 104 comprises a printing device, and in particular,
5 an IPP-compliant printer. However, the invention is not limited for use with networked printers (IPP-compliant or otherwise), but instead can be used to provide access to any of a variety of data communication devices, including facsimile machines, image servers and file servers. Further, the invention is not limited for use with land-based data communications devices, but instead can be used to provide
10 access to wireless communications devices. For instance, the network resource control system 100 can be configured to facilitate data communication with e-mail pagers or e-mail enabled wireless telephones.

It is expected that some of the network resources 104 may be located behind an
15 enterprise firewall. Accordingly, to facilitate communication between network terminals 200 and firewall-protected network resources 104, the network resource control system 100 may also include a proxy server 114 located logically outside the enterprise firewall, and a polling server 116 located logically within the firewall, as shown in Fig. 1. Preferably, the proxy server 114 is located on-site at the enterprise
20 responsible for administering the network resource 104, is provided with a network address corresponding to the enterprise, and includes a queue for receiving application data. However, the proxy server 114 may also be located off-site, and may be integrated with the authorization server 110 if desired. This latter option is advantageous since it allows system administrators to provide access to network
25 resources 104, but without having to incur the expense of the domain name registration and server infrastructure.

In addition to the proxy server 114 and the polling server 116, preferably the enterprise includes an enterprise server 118 (eg. a print server) to facilitate
30 communication with the network resources 104 located behind the firewall. The polling server 116 is in communication with the enterprise server 118, and is configured to periodically poll the proxy server 114 through the firewall to determine whether application data from a network terminal 200 is waiting in the queue of the proxy server 114. The proxy server 114 is configured to transmit any queued

application data to the polling server 116 in response to the poll signal from the polling server 116. Upon receipt of the queued application data from the proxy server 114, the polling server 116 transmits the application to the enterprise server 118 for distribution to the appropriate network resource 104. As will be apparent, this
5 mechanism allows application data to be transmitted to network resources 104 located behind a firewall, but without exposing the enterprise to the significant possibility of security breaches associated with firewall access ports.

The resource registry 106 comprises a resource database 120, a driver database 122,
10 and a user registration database 124. The resource database 120 includes resource records 300 identifying parameters associated with the network resources 104. As shown in Fig. 3, each resource record 300 comprises a network address field 302, a resource type field 304, and a user access level field 306 for the associated network resource 104. The network address field 302 identifies the network address of the
15 network resource 104. As discussed above, typically each network resource 104 comprises an IPP-compliant printer, in which case the network address field 302 identifies comprises the network resource IPP address. However, in the case where the network resource 104 comprises a non-IPP-compliant device and the communications network 112 comprises the Internet, preferably the network resource
20 104 is linked to the communications network 112 via a suitable server, and the network address field 302 for the network resource 104 identifies the Internet Protocol ("IP") address of the server.

The resource type field 304 identifies the type of data communication device of the
25 network resource 104. For instance, the resource type field 304 may specify that the network resource 104 is a printer, an image server, a file server, an e-mail pager, or an e-mail enabled wireless telephone. Further, the resource type field 304 may include a resource type sub-field specifying a sub-class of the network resource type. For example, the resource type sub-field may specify that the network resource 104 is an
30 IPP-capable printer, or a non-IPP-capable printer.

The user access level field 306 identifies the type of communications access which the network terminals 200 are allowed to have in regards to the associated network

resource 104. In the embodiment, as presently envisaged, the user access level field 306 establishes that the network resource 104 allows one of:

- 5 (a) "public access" in which any network terminal 200 of the network resource control system 100 can communicate with the network resource 104;
- (b) "private access" in which only members (eg. employees) of the enterprise associated with the network resource 104 can communicate with the network resource 104; and
- 10 (c) "authorized access" in which only particular network terminals 200 can communicate with the network resource 104.

If the user access level field 306 specifies "authorized access" for a network resource 104, preferably the user access level field 306 includes a sub-field which lists the
15 names of the network terminals 200 authorized to access the network resource 104, and a sub-field which includes an authorization password which the identified network terminals 200 must provide in order to access the network resource 104. If the user access level field 306 specifies "private access" for a network resource 104, preferably the user access level field 306 includes a sub-field which lists the network
20 address of the network terminals 200 which are deemed to members of the enterprise.

It should be understood, however, that the user access level field 306 is not limited to identifying only the foregoing predefined user access levels, but may instead identify more than one of the predefined user access levels, or other user access levels
25 altogether. For instance, the user access level field 306 may identify that the associated network resource 104 allows both private access to all employees of the enterprise running the network resource 104, and authorized access to other pre-identified network terminals 200. Further, the user access level field 306 may also include one or more sub-fields (not shown) which provide additional
30 restrictions/permissions on the type of communications access which the network terminals 200 are allowed to have in regards to the associated network resource 104. For instance, the user access level sub-fields may limit the hours of operation of the network resource 104, or may place restrictions on the type of access limitations on a per-user basis, or per-group basis. Other variations on the type of access will be

readily apparent, and are intended to be encompassed by the scope of the present invention.

5 Preferably, each resource record 300 includes an information field 308 which provides information on the network resource 104, such as data handling capabilities, resource pricing and geographical co-ordinates. This latter parameter is particularly advantageous for use with mobile network terminals 200, such as a wireless-enabled personal data assistant or an e-mail-enabled wireless telephone, since it allows the network terminal 200 to identify the nearest one of a plurality of available network
10 resources 104. This aspect of the invention will be explained in greater detail below.

Each resource record 300 also includes a pseudo-name field 310, a username/password field 312 and a network driver identifier field 314. The pseudo-name field 310 contains a resource pseudo-name which identifies the network
15 resource 104 to the network terminals 200. Preferably, the pseudo-name is a network alias that identifies the physical location and properties of the network resource 104, but does not identify the network address of the resource 104. Further, preferably each pseudo-name uniquely identifies one of the network resources 104, however a group of the network resources 104 may be defined with a common pseudo-name to
20 allow communication with a group of network resources 104. This latter feature is particularly advantageous since it allows the administrator of an enterprise associated with the group of network resources to dynamically allocate each network resource 104 of the group as the demands for the network resources 104 or maintenance schedules require.

25 In addition, preferably the resource record 300 includes a plurality of the pseudo-name fields 310 to allow the administrator of the associated network resource 104 to update the name assigned to the network resource 104, while also retaining one or more previous pseudo-names assigned to the network resource 104. As will be
30 explained, this feature is advantageous since it allows the administrator to update a resource name without the risk that network terminals 200 using a prior pseudo-name will be unable to locate or communicate with the network resource 104.

5 The username/password field 312 contains a unique username and password combination which allows the administrator of the associated network resource 104 to prevent authorized access and alteration to the data contained in the resource record 300. Preferably, each resource record 300 also includes an e-mail address field (not shown) which the network resource control system 100 uses to provide the administrator of the associated network resource 104 with a notification e-mail message when a message is successfully transmitted to the network resource 104.

10 The driver identifier field 314 contains a resource driver identifier which is used in conjunction with the driver database 122 to provide the network terminals 200 with the appropriate resource driver for communication with the network resource 104. The driver database 122 includes resource drivers which allow software applications installed on the network terminals 200 to communicate with the network resources 104. As will be explained below, in order for a network terminal 200 to communicate
15 with a selected network resource 104, the network terminal 200 first downloads a driver application data from the administration server 108 over the communications network 112. The network terminal 200 may also download the appropriate resource driver from the driver database 122 (via the authorization server 110 over the communications network 112), and then allow the authorization server 110 to
20 configure the downloaded resource driver in accordance with the access level field 306 of the resource record 300 associated with the selected network resource 104. Preferably, each resource driver includes a resource driver identifier which allows the authorization server 110 to identify the resource driver which the network terminal 200 has downloaded.

25

The driver application will now be discussed in association with Fig. 2. As discussed above, the DISC 210 of the network terminal 200 includes data which, when loaded into the RAM 212 of the network terminal 200, comprise processor instructions for the CPU 208. As shown, the downloaded driver application data defines in the RAM
30 212 a memory object comprising a driver application 400. The driver application 400 includes a generic resource driver 402 and a wrap-around resource driver layer 404. The generic resource driver 402 allows the network terminal 200 to communicate with a variety of different network resources 104, however the generic resource driver 402 typically will not provide the network terminal 200 with access to all the features and

capabilities of any particular network resource 104. If the network terminal 200 requires additional features not implemented with the generic resource driver 402, the appropriate resource driver may be downloaded from the driver database 116, as mentioned above.

5

The wrap-around driver layer 404 includes an application communication layer 406, a driver administrator layer 408, and a data transmitter layer 410. The application communication layer 406 is in communication with the resource driver 402 (generic or network resource specific) and the application software installed on the network terminal 200, and is configured to transmit user application data between the application software and the resource driver 402. The driver administrator layer 408 communicates with the resource registry 106 over the communications network 112 to ensure that the driver application 400 is properly configured for communication with the selected network resource 104. The data transmitter layer 410 is in communication with the resource driver 402 and is configured to transmit the data output from the resource driver 402 over the communications network 112 to the selected network resource 104, via the network interface 202. Although the driver application 400 and its constituent component layers are preferably implemented as memory objects or a memory module in the RAM 212, it will be apparent that the driver application 400 may instead be implemented in electronic hardware, if desired.

Returning to Fig. 1, the registration database 124 of the resource registry 106 includes user records each uniquely associated with a user of a respective network terminal 200 upon registration with the network resource control system 100. Each user record identifies the name the registered user's name, post office address and e-mail address. In addition, each user record specifies a unique password which the registered user must specify in order to update the user's user record, and to obtain access to network resources 104 configured for "authorized access". The user record may also include additional information specifying default options for the network resource control system 100. For instance, the user may specify that the network resource control system 100 should provide the user with an acknowledgement e-mail message when a message is successfully transmitted to a selected network resource 104. The user may also specify an archive period for which the network resource control system 100 should archive the message transmitted to the selected network resource 104. This

latter option is advantageous since it allows the user to easily transmit the same message to multiple network resources 104 at different times, and to periodically review transmission dates and times for each archive message.

5 The administration server 108 is in communication with the resource database 120 and the registration database 124. The administration server 108 provides administrators of the network resources 104 with access to the records of the resource database 120 to allow the administrators to update the network address field 302, the resource type field 304, the user access level field 306, the resource information field 10 308, the pseudo-name field 310, the username/password field 312 and/or the driver identifier field 314 of the resource record 300 for the associated network resource 104. As will become apparent, this mechanism allows network administrators to change, for example, the network address and/or the restrictions/permissions of the network resources 104 under their control, or even the network resource 104 itself, without 15 having to notify each network terminal 200 of the change. The administration server 108 also provides controlled access to the registration database 124 so that only the user of the network terminal 200 which established the user record can update the user record.

20 Where the username/password field 312 has been completed, the administration server 108 is configured to block access to the resource record 300 until the administrator provides the administration server 108 with the correct username/password key. This feature allows the resource administrator to make adjustments, for example, to pricing and page limit, in response to demand for the 25 network resources 104, and to make adjustments to the restrictions/permissions set out in the user access level field 306 and the resource information field 308 and thereby thwart unauthorized access to the network resources 104.

30 The authorization server 110 is in communication with the resource database 120 and the driver database 122 for providing the network terminals 200 with the resource drivers 402 appropriate for the selected network resources 104. Preferably, the authorization server 110 is also configured to configure the driver application 400 for communication with the selected network resource 104, by transmitting the network address of the selected network resource 110 to the data transmitter layer 410 over a

-12-

communications channel secure from the user of the network terminal 200 so that the network address of the network resource 104 is concealed from the user of the network terminal 200. In the case where the communications network 112 comprises the Internet, preferably the secure communications channel is established using the

5 Secure Sockets Layer ("SSL") protocol.

In addition to the network terminal 200, the network resource 104, the resource registry 106, the administration server 108, the authorization server 110, and the communications network 112, preferably the network resource control system 100

10 also includes a transaction server 126 and an archive server 128. The transaction server 126 is in communication with the authorization server 110 for keeping track of each data transfer between a network terminal 200 and a network resource 104. For each transmission, preferably the transaction server 126 maintains a transmission record identifying the network terminal 200 which originated the transmission, the

15 network resource 104 which received the transmission, and the date, time and byte size of the transmission.

The archive server 128 is configured to retain copies of the data transmitted, for a specified period. As discussed above, the user of a network terminal 200 specifies the

20 requisite archive period (if any) for the data transmission, upon registration with the network resource control system 100. Preferably, the administration server 108 provides controlled access to the transaction server 126 and the archive server 128 so that only the user of the network terminal 200 which originated transmission of the data is allowed access to the transmission record associated with the transmission.

25

The process by which a user of a network terminal 200 can communicate with a network resource 104 will now be described with reference to Fig. 4. The following discussion presupposes that the user of the network terminal 200 has downloaded the driver application 400 from the administration server 108 over the communications

30 network 112. At step 500, the user of a network terminal 200 decides whether to log in to the network resource control system 100. As discussed above, if the user registers with the network resource control system 100 and subsequently logs in to the network resource control system 100 (by providing the authorization server 106 with the user's assigned password), the user will have access to any network resources 104

-13-

which have "authorized access" as the user access level and which have identified the registered user as a user authorized to access the network resource 104. If the user does not register or fails to log in to the network resource control system 100, the user will only have access to network resources 104 which have established "public access" as the user access level.

At step 502, the user selects a network resource 104 by querying the administration server 108 for a list of available network resources 104. Alternately, the user may postpone selection of a network resource 104 until initiation of the transmission command. The network user query may be based upon any desired criteria, including print turn-around time and page size (where the target network resource 104 is a printer), price, and geography. In addition, the user may provide the administration server 108 with the geographical coordinates of the user to determine the user's nearest network resources. The user may provide its geographical coordinates through any suitable mechanism known to those skilled in the art, including latitude/longitude co-ordinates, GPS, and wireless triangulation.

If the user requested a list of available network resources 104, the user is provided with a list of pseudo-names associated with each network resource 104 satisfying the designated search criteria. As discussed above, if the user logged in to the network resource control system 100, the pseudo-name list will include both "public access" network resources 104 and "authorized access" network resources 104 with which the user has been authorized to communicate. Also, if the user is member of an enterprise having network resources 104 registered with the network resource control system 100, the pseudo-name list will also identify network resources 104 which have been registered by the enterprise for "private access". Otherwise, the pseudo-name list will only identify network resources 104 registered for public access. Upon receipt of the resource list, the user selects a network resource 104 from the list.

At step 504, the administration server 108 queries the network user's network terminal 200 for the resource driver identifier of the resource driver 402 configured on the network terminal 200, and then compares the retrieved resource driver identifier against the resource driver identifier specified in the network driver identifier field 314 of the resource record 300 associated with the selected network resource 104 to

-14-

determine whether the driver application 400 has been configured with the appropriate resource driver 402 for communication with the network resource 104. If the network terminal 200 has not been configured with the appropriate resource driver 402, the administration server 108 prompts the user's network terminal 200 to download the necessary resource driver 402. As will be apparent, the downloaded resource driver 402 becomes part of the driver application 400.

When the user of the network terminal 200 is ready to communicate with the selected network resource 104, the user of the network terminal 200 transmits a transmission request via its application software to the driver application 400, at step 506. If the user did not select a network resource 104 at step 502, the application communication layer 406 of the driver application 400 contacts the administration server 108 over the communications network 112 and prompts the user to select a network resource 104, as described above. Once a network resource 104 is selected, and the appropriate resource driver 402 is installed, the application communication layer 406 notifies the driver administrator layer 408 of the transmission request.

At step 508, the driver administrator layer 408 provides the authorization server 110 with the transmission request and identifies the selected network resource 104, by transmitting to the authorization server 110 the pseudo-name assigned to the selected network resource 104. If the user of the network terminal 200 has registered and logged in to the network resource control system 100, the driver administrator layer 408 also provides the authorization server 110 with the registered user's name.

The authorization server 110 then queries the resource database 120 with the received pseudo-name for the resource record 300 associated with the pseudo-name, at step 510. The authorization server 110 then extracts the user access level from the user access level field 306 of the retrieved resource record 300, and determines whether the network terminal 200 is authorized to communicate with the selected network resource 104, at step 512. As will be apparent from the foregoing discussion, if the user access level field 306 specifies "public access" for the network resource 104, the network terminal 200 will be automatically authorized to communicate with the network resource 104.

However, if the user access level field 306 specifies "private access" for the network resource 104, the authorization server 110 determines the network address of the network terminal 200 from the transmission request transmitted by the network terminal 200, and then queries the user access level sub-field with the terminal's network address to determine whether the network terminal 200 is authorized to communicate with the network resource 104. In the case where the communications network 112 comprises the Internet, the authorization server 110 can determine the network terminal's network address from the IP packets received from the network terminal 200. On the other hand, if the user access level field 306 specifies "authorized access" for the network resource 104, the authorization server 110 queries the user access level sub-field with the user's name to determine whether the network terminal 200 is authorized to communicate with the network resource 104.

If the query at step 512 reveals that the network terminal 200 is not authorized to communicate with the network resource 104, at step 514 the authorization server 110 provides the network terminal 200 with a notification that the network terminal 200 is not authorized for communication with the selected resource 104. However, if the query at step 512 reveals that the network terminal 200 is authorized to communicate with the network resource 104, the authorization server 110 queries the network address field 302 of the resource record 300 associated with the network resource 104 for the network address of the network resource 104. The authorization server 110 then establishes a secure communications channel with the driver administrator layer 408, and then transmits the network address to the driver administrator layer 408 over the secure communications channel, at step 516.

Also, if the user access level field 306 specifies "authorized access" for the network resource 104, and the network terminal 200 is authorized to communicate with the network resource 104, the authorization server 110 queries the user access level sub-field for the authorization password assigned to the network resource 104, and then transmits the authorization password to the driver administrator layer 408 over the secure communications channel, together with the network address. In the case where the communications network 112 comprises the Internet, preferably the authorization server 110 establishes the secure communications channel using a Secure Sockets Layer ("SSL") protocol. Since the network address and the authorization password

-16-

are transmitted over a secure communications channel, this information is concealed from the user of the network terminal 200.

5 Preferably, the authorization server 110 also extracts the resource driver identifier from the resource identifier field 314 of the resource record 300, and determines whether the network terminal 200 is still properly configured for communication with the network resource 14. If the network terminal 200 no longer has the correct resource driver 402, the authorization server 110 queries the driver database 122 for the correct resource driver 402, and prompts the user of the network terminal 200 to
10 download the correct resource driver 402. This driver configuration verification step may be performed concurrently or consecutively with the network address providing step described in the preceding paragraph.

15 In addition, the administration server 108 queries the registration database 124 to determine whether the user of the network terminal 200 registered with the network resource control system 100. If the user registered with the network resource control system 100 and specified that the archive server 128 should maintain archival copies of data transmissions, the administration server 108 transmits the network address of the archive server 128 to the driver administrator layer 408. As a result, when the user
20 of the network terminal 200 issues a data transmission command, the driver application 400 will transmit the user application data to the selected network resource 104 and to the archive server 128.

25 At step 518, the application communication layer 406 passes the application data received from the application software to the resource driver 402 for translation into a format suitable for processing by the selected network resource 104. Meanwhile, the driver administrator layer 408 interrogates the network resource 104, using the received network address, to determine whether the network resource 104 still resides at the specified network address, is operational and is on-line.

30

If the interrogated network resource 104 resides at the specified network address, is operational and is on-line. online, the resource driver 202 passes the translated application data to the data transmitter layer 410 of the driver application 400. Preferably, the data transmitter layer 410 compresses and encrypts the translated

-17-

application data upon receipt. The data transmitter layer 410 also receives the network address of the network resource 104 from the driver administrator layer 408, adds the network address data to the compressed, encrypted data, and then transmits the resulting data over the communications network 112 to the network resource 104 at the specified network address, at step 520.

Preferably, the data transmitter layer 410 also transmits details of the transmission to the transaction server 126, such as the selected network resource 104 and the byte size of the transmission. Upon receipt of the transmission details, preferably the administration server 108 queries the resource database 120 and the user registration database 124 for the e-mail address of the resource administrator and the e-mail address of the user of the network terminal 200, if provided, and then transmits an e-mail message indicating completion of the transmission.

If the user access level field 306 specifies "authorized access" for the network resource 104, the data transmitter layer 410 also receives the authorization password for the network resource 104 from the driver administrator layer 408, and transmits the authorization password (as part of the compressed, encrypted data) to the network resource 104.

If the user access level field 306 specifies "public access" for the network resource 104, preferably the network resource 104 is accessible through a local server which serves to queue, decrypt and decompress the application data, and extract the network address data, and then transmit the decompressed application data to the appropriate network resource 104. Alternately, the network resource 104 itself may be configured for direct communication over the communications network 112, such as an IPP-capable printer, so that the network resource 104 is able to process the application data directly.

If the user access level field 306 specifies "authorized access" for the network resource 104, preferably the network resource 104 is accessible through a local server which serves to queue, decrypt and decompress the application data, and extract the network address data and authorization password, and then transmit the application

-18-

data to the appropriate network resource 104 if the received authorization password is valid.

If the user access level field 306 specifies "private access" for the network resource 104, typically the network resource 104 will be located behind a firewall.

Accordingly, the proxy server 114 associated with the network resource 104 will receive the application data, and transfer the application data to the proxy server queue. The polling server 116 associated with the network resource 104 will poll the proxy server 114 to determine the status of the queue. Upon receipt of a polling signal from the polling server 116, the proxy server 114 transmits any queued application data from the proxy server queue, through the firewall, to the polling server 116. The polling server 116 then extracts the network address from the received application data, and transmits the application data to the appropriate server 118 or network resource 104 for processing.

As will be apparent from the foregoing discussion, regardless of the user class defined for a network resource 104, if a resource administrator relocates a network resource 104 to another network address, and/or changes the device type and/or restrictions/permissions associated with the network resource 104, the resource administrator need only update the resource record 300 associated with the network resource 104 to continue communication with the network resource 104.

Subsequently, when a user attempts communication with the network resource 104 using the original pseudo-name, the authorization server 110 will provide the administrator layer 408 with the updated network address of the network resource 104, or prompt the user to download the appropriate resource driver 402, assuming that the network terminal 200 is still authorized to communicate with the network resource 104.

Further, if the user access level field 306 specifies "authorized access" for the network resource 104 and the resource administrator desires to change the pseudo-name and authorization password associated with the network resource 104, the resource administrator need only update the pseudo-name and authorization password provided on the resource record 300. Subsequently, when a user of a network terminal 200 initiates communication with the network resource 104 using the original pseudo-

-19-

name, the authorization server 110 scans the resource records 300 for occurrences of the original pseudo-name. After locating the appropriate resource record 300, the authorization server 110 provides the driver administrator layer 408 with the updated pseudo-name and authorization password of the network resource 104, provided that

5 the network terminal 200 is still authorized to communicate with the network resource 104. A network terminal 200 which is not authorized to communicate with the network resource 104 will not receive the updated pseudo-name and authorization password from the authorization server 110 and, consequently, will not be able to communicate with the network resource 104, even if the user of the network terminal

10 200 knew the network address for the network resource 104.

The foregoing description is intended to be illustrative of the preferred embodiment of the present invention. Those of ordinary skill may envisage certain additions, deletions and/or modifications to the described embodiment which, although not

15 explicitly described herein, are encompassed by the spirit or scope of the invention, as defined by the claims appended hereto.

WE CLAIM:

1. A network resource control system for facilitating communication between network terminals and network resources over a network, the network resource control system comprising:
 - a resource registry including resource records associated with the network resources, the resource records defining at least a user access level for each said network resource;
 - an authorization server in communication with the resource registry for controlling network access to the network resources by the network terminals in accordance with the resource records; and
 - an administration server in communication with the resource registry for providing controlled access to the resource records.
2. The network resource control system according to claim 1, wherein the resource records define at least resource configuration data for each said network resource, and each said network terminal has an associated terminal configuration, and the authorization server is configured to receive from one of the network terminals a request for access to one of the network resources, and to configure the one terminal for communication with the one network resource in accordance with a correspondence between the terminal configuration of the one network terminal and the resource configuration data and the user access control data associated with the one network resource.
3. The network resource control system according to claim 2, wherein the authorization server is configured to provide the one terminal with a network resource driver for communication with the one network resource in accordance with the correspondence.
4. The network resource control system according to claim 1, wherein the resource records are configured for access by respective administrators of the network resources, and the administration server is configured to receive from one of the network administrators a request for access to one of the resource records with user access control data, to verify authorization for the access from the access configuration associated with the one resource record, and to update the one resource record with the user access control data in accordance with the verification.

5. A method for facilitating communication between network terminals and network resources over a network, the method comprising the steps of:

providing a resource registry including resource records associated with the network resources;

receiving user access control data from administrators of the network resources for incorporation into the resource records; and

in accordance with the user access control data, configuring the network terminals for communication with the network resources.

6. The method according to claim 5, wherein the resource records define at least resource configuration data for each said network resource, and each said network terminal has an associated terminal configuration, and the terminal configuring step comprises the steps of receiving from one of the network terminals a request for access to one of the network resources, and configuring the one terminal for communication with the one network resource in accordance with a correspondence between the terminal configuration of the one network terminal and the resource configuration data and the user access control data associated with the one network resource.

7. The method according to claim 6, wherein the step of configuring the one terminal comprises providing the one terminal with a network resource driver for communication with the one network resource in accordance with the correspondence.

8. The method according to claim 5, wherein each said resource record is configured for access by one of the network administrators, and the control data receiving step comprises the steps of receiving from one of the network administrators a request for access to one of the resource records, verifying authorization for the access from the access configuration associated with the one resource record, and updating the one resource record in accordance with the verification.

1/5

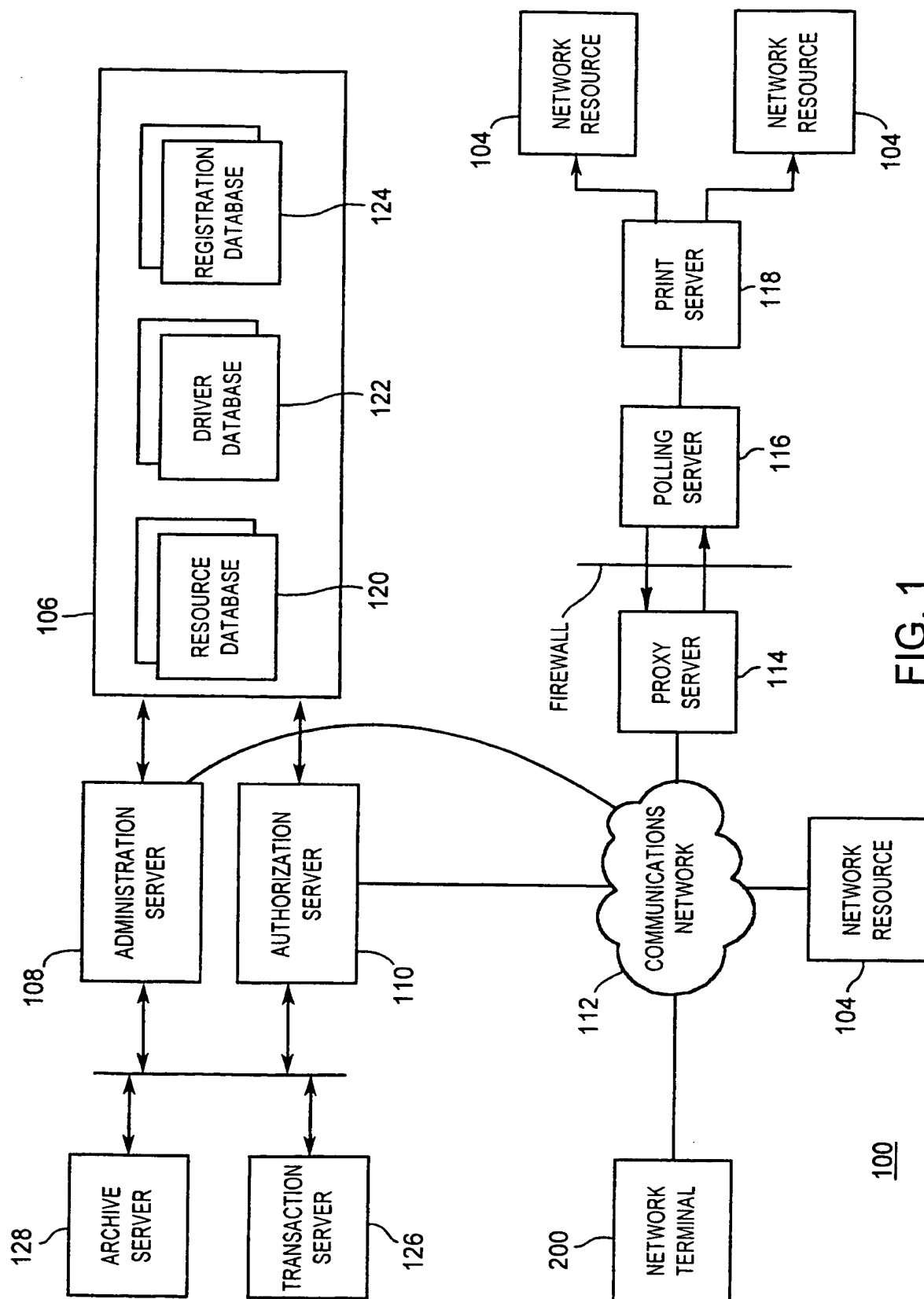


FIG. 1

2/5

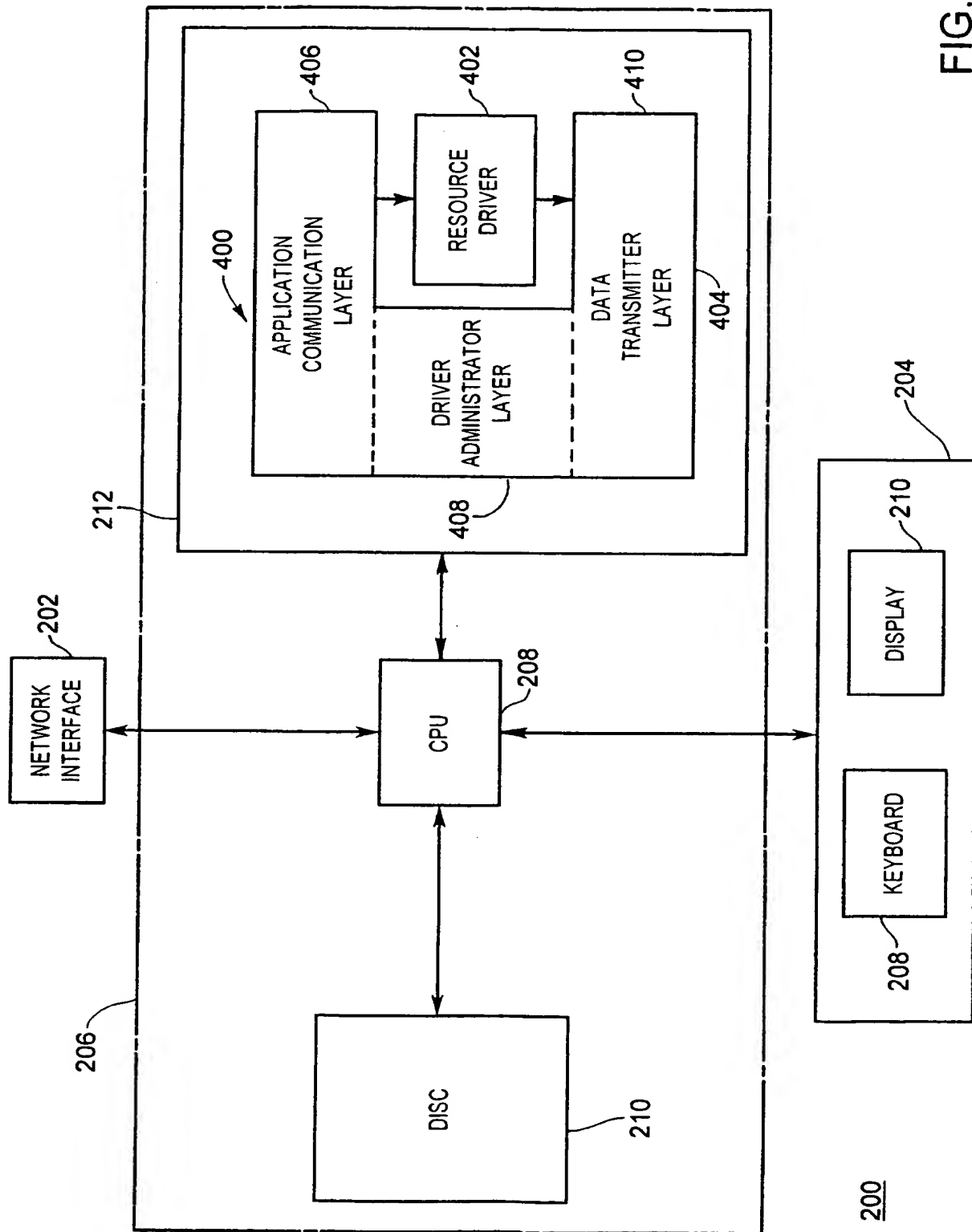
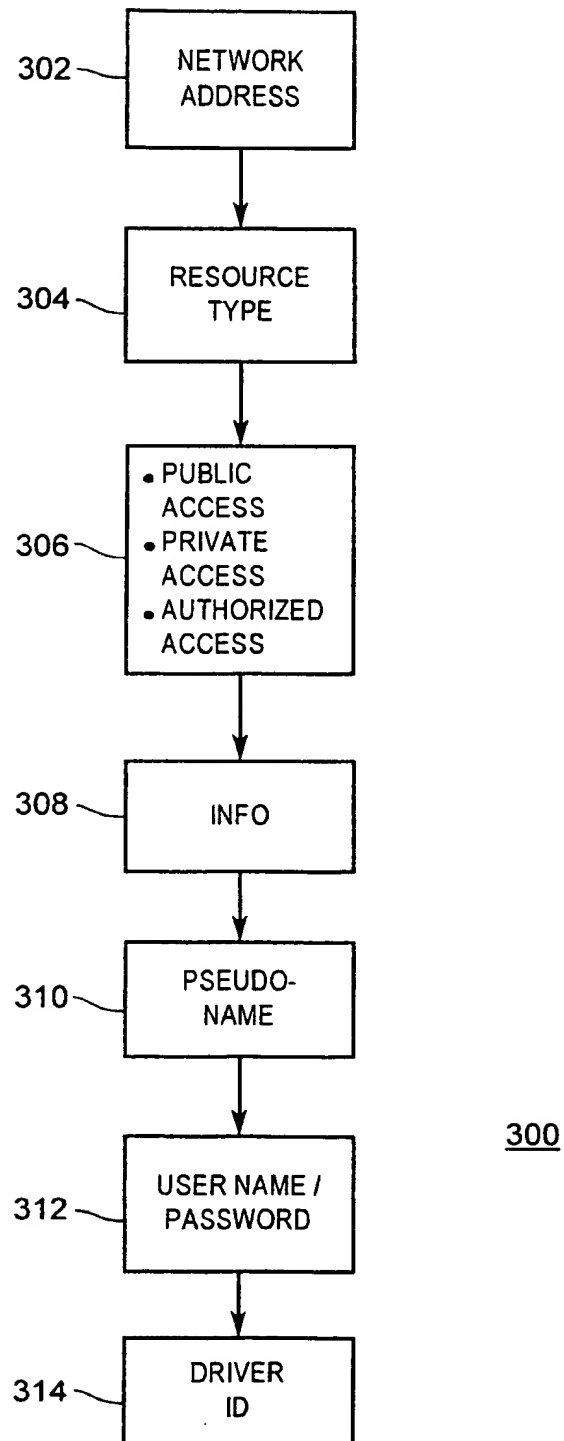
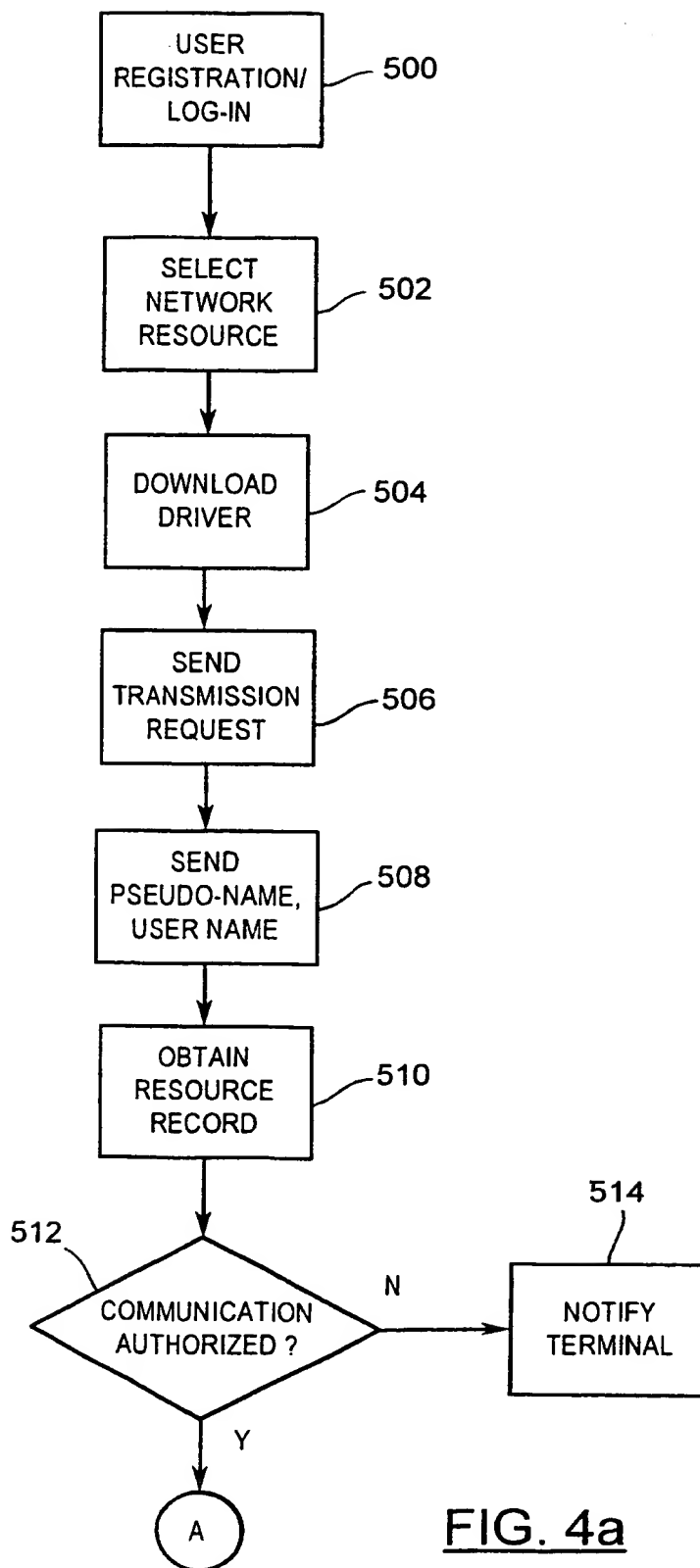


FIG. 2

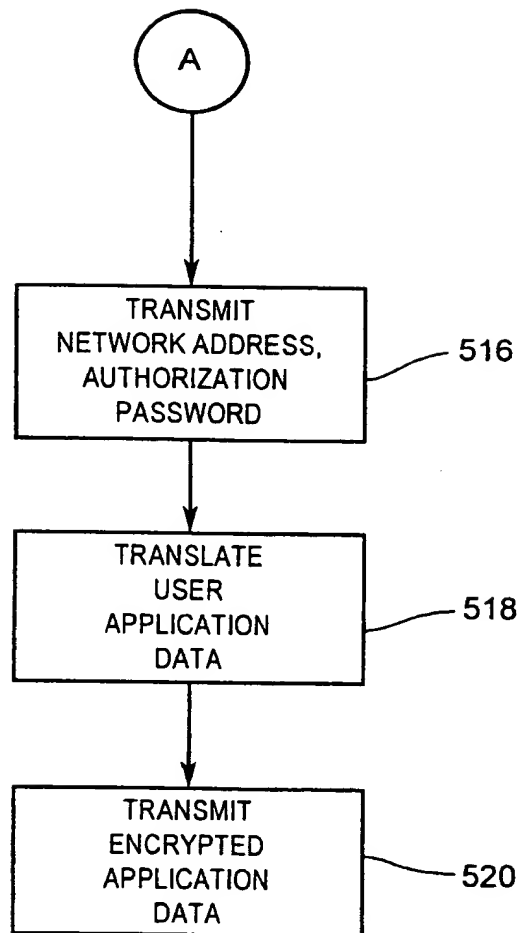
3/5

FIG. 3

4/5

FIG. 4a

5/5

FIG. 4b

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.